IKEv2 および証明書を使用した IOS Headend Over IPsec に対する AnyConnect の設定例

内容

概要

このドキュメントでは、FlexVPN フレームワークを利用して証明書認証のみで AnyConnect クライアントを実行しているデバイスから Cisco IOS® ルータへの IPsec で保護された接続を実現する方法を説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FlexVPN

- AnyConnect

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

ヘッドエンド

Cisco IOS ルータには、IKEv2 を実行可能で、15.2 M&T 以上のリリースを実行するどのルータでも使用できます。ただし、可能な場合は最新リリースを使用する必要があります（既知の注意事項に関するセクションを参照）。

クライアント

AnyConnect 3.x リリース

認証局

この例では、認証局（CA）は 15.2(3)T リリースを実行します。

Extended Key Usage（EKU）をサポートする必要があるため、いずれかの最新リリースを使用することが重要です。

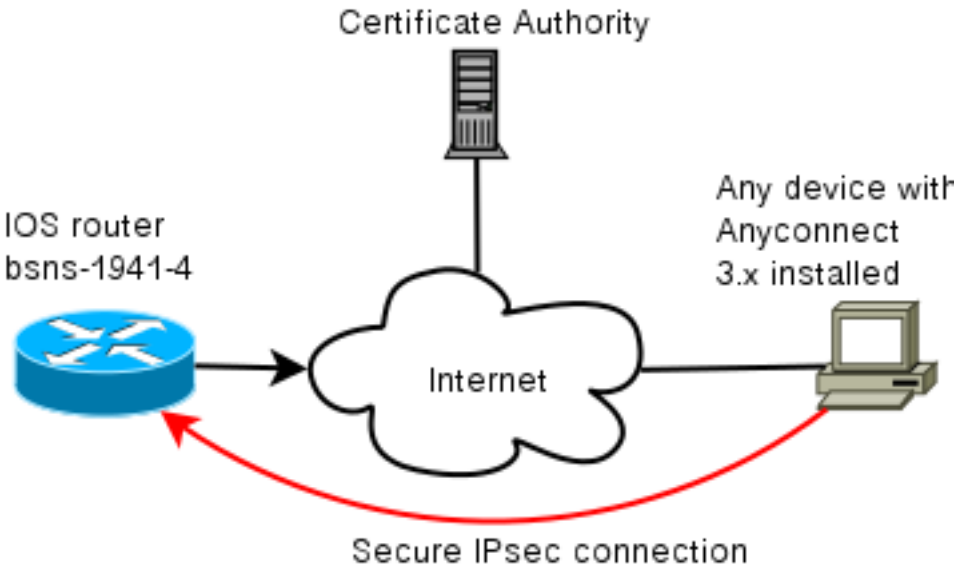
この導入では、CA として IOSルータが使用されます。ただし、EKU が使用できれば、どの標準ベース CA アプリケーションでも問題ありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

コンフィギュレーション

Network Topology



認証局（オプション）

認証局の使用を選択した場合、IOS ルータは CA としても機能します。

IOS CA の設定

CA サーバではクライアントとサーバの証明書に正しい EKU を設定しなければならないことを覚えておく必要があります。この例では、server-auth および client-auth EKU がすべての証明書に設定されています。

```
bsns-1941-3#show run | s crypto pki
crypto pki server CISCO
database level complete
database archive pem password 7 00071A1507545A545C
issuer-name cn=bsns-1941-3.cisco.com,ou=TAC,o=cisco
grant auto rollover ca-cert
grant auto
auto-rollover
eku server-auth client-auth
```

適切な EKU が証明書に設定されているかどうかを確認する方法

bsns-1941-3 は CAサーバで、bsns-1941-4 は IPsec のヘッドエンドです。簡略化のため、出力の一部を省略しています。

```
BSNS-1941-4#show crypto pki certificate verbose
Certificate
(...omitted...)

Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: C3D52BE9 1EE97559 C7323995 3C51DC53
Fingerprint SHA1: 76BC7CD4 F298F8D9 A95338DC E5AF7602 9B57BE31
X509v3 extensions:
X509v3 Key Usage: A0000000
```

```
Digital Signature
Key Encipherment
X509v3 Subject Key ID: 83647B09 D3300A97 577C3E2C AAE7F47C F2D88ADF
X509v3 Authority Key ID: B3CC331D 7159C3CD 27487322 88AC02ED FAF2AE2E
Authority Info Access:
Extended Key Usage:
Client Auth
Server Auth
Associated Trustpoints: CISCO2
Storage: nvram:bsns-1941-3c#5.cer
Key Label: BSNS-1941-4.cisco.com
Key storage device: private config

CA Certificate
(...omitted...)
```

ヘッドエンドの設定

ヘッドエンドの設定は 2 つの部分で構成されています。それは、PKI 部分と実際の flex/IKEv2 です。

PKI 設定

bsns-1941-4.cisco.com の CN が使用されていることがわかります。これは適切な DNS エントリと一致し、AnyConnect プロファイルの <Hostname> に含まれている必要があります。

```
crypto pki trustpoint CISCO2
enrollment url http://10.48.66.14:80
serial-number
ip-address 10.48.66.15
subject-name cn=bsns-1941-4.cisco.com,ou=TAC,o=cisco
revocation-check none

crypto pki certificate map CMAP 10
subject-name co cisco
```

暗号化と IPsec の設定

提案の PRF/integrity 設定は、証明書がサポートする内容と一致する**必要があることに注意してください。**これは通常 SHA-1 です。

```
crypto ikev2 authorization policy AC
pool AC

crypto ikev2 proposal PRO
encryption 3des aes-cbc-128
integrity sha1
group 5 2

crypto ikev2 policy POL
match fvrf any
proposal PRO

crypto ikev2 profile PRO
match certificate CMAP
```

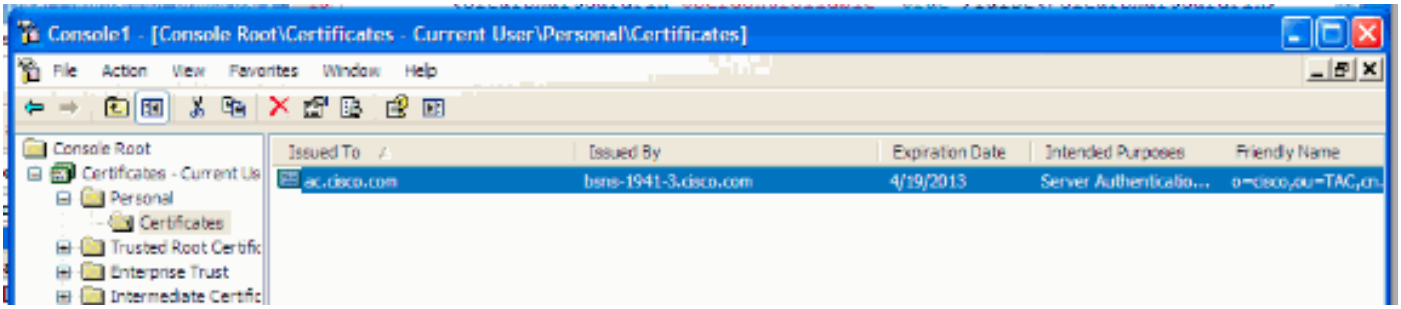
```
identity local dn
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint CISCO2
aaa authorization group cert list default AC
virtual-template 1

no crypto ikev2 http-url cert
crypto ipsec transform-set TRA esp-3des esp-sha-hmac

crypto ipsec profile PRO
set transform-set TRA
set ikev2-profile PRO

interface Virtual-Template1 type tunnel
ip unnumbered GigabitEthernet0/0
tunnel mode ipsec ipv4 tunnel protection ipsec profile PRO
```

クライアント

IKEv2 および証明書と AnyConnect が正常に接続するためのクライアント設定は 2 つの部分で構成されています。

証明書登録

証明書を正しく登録すると、マシンまたはパーソナル ストアに証明書があることを確認できます。クライアント証明書には EKU を設定する必要もあります。



AnyConnect プロファイル

AnyConnect プロファイルは長く、非常に基本的です。

関連部分では、以下を定義します。

1. 接続しているホスト
2. プロトコルのタイプ
3. そのホストへの接続時に使用する認証

使用内容は次のとおりです。

```
<ServerList>
<HostEntry>
<HostName>bsns-1941-4.cisco.com</HostName>
<PrimaryProtocol>IPsec
```

```
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>
IKE-RSA
</AuthMethodDuringIKENegotiation>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

AnyConnect の接続フィールドでは、完全な FQDN を指定する必要があります。FQDN は <HostName> に示されている値です。

接続の検証

簡略化のため一部の情報は省略されています。

```
BSNS-1941-4#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA
Tunnel-id Local Remote fvrf/ivrf Status
2    10.48.66.15/4500    10.55.193.212/65311   none/none    READY
Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:5,
Auth sign: RSA, Auth verify: RSA
Life/Active Time: 86400/180 sec


IPv6 Crypto IKEv2 SA

BSNS-1941-4#show crypto ipsec sa

interface: Virtual-Access1
Crypto map tag: Virtual-Access1-head-0, local addr 10.48.66.15

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/0/0)
current_peer 10.55.193.212 port 65311
PERMIT, flags={origin_is_acl,}
#pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
#pkts decaps: 26, #pkts decrypt: 26, #pkts verify: 26

local crypto endpt.: 10.48.66.15, remote crypto endpt.: 10.55.193.212
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0x5C171095(1545015445)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8283D0F0(2189676784)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel UDP-Encaps, }
conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000040,
crypto map: Virtual-Access1-head-0
sa timing: remaining key lifetime (k/sec): (4215478/3412)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound esp sas:
spi: 0x5C171095(1545015445)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel UDP-Encaps, }
```

```
conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000040,
crypto map: Virtual-Access1-head-0
sa timing: remaining key lifetime (k/sec): (4215482/3412)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

次世代暗号化

上記の構成は、最小限の動作をするための設定を示すための参照として提供されています。可能な場合は次世代暗号化（NGC）を使用することをお勧めします。

移行の現在の推奨事項は、以下を参照してください。
http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

NGC 設定を選択するときに、クライアント ソフトウェアとヘッドエンド ハードウェアの両方がその設定をサポートすることを確認します。NGC のハードウェア サポートがあるため、ISR Generation 2 と ASR 1000 ルータをヘッドエンドとしてお勧めします。

AnyConnect 3.1 バージョンの時点では、AnyConnect 側で NSA の Suite B アルゴリズム スイートがサポートされます。

既知の注意事項と問題

- IOS ヘッドエンドには**no crypto ikev2 http-url cert** の行を設定してください。この行が設定されない場合に IOS ソフトウェアと AnyConnect で生成されるエラーは誤解を招きます。
- IKEv2 セッションを使用する初期の IOS 15.2M&T ソフトウェアは RSA-SIG 認証に対して起動しない場合があります。これは Cisco bug ID CSCtx31294 に関連する可能性があります（登録ユーザ専用）。 最新の 15.2M または 15.2T ソフトウェアを実行してください。
- 特定のシナリオで、 IOS は認証する適切なトラストポイントを選択できない場合があります。シスコはこの問題を把握しており、15.2(3)T1 および 15.2(4)M1 リリースで修正されています。
- AnyConnect で次のようなメッセージが示される場合、

```
The client certificate's cryptographic service provider(CSP)
does not support the sha512 algorithm
```

IKEv2 提案の integrity/PRF 設定が証明書で処理できる内容と一致しているか確認する必要があります。上記の設定例では、SHA-1 が使用されています。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems